[redacted]

Talon

Information in this document, including attachments and exhibits, is subject to the International Traffic in Arms Regulations (ITAR) or Export Administration Regulations (EAR). No information from this document may be exported, released or disclosed to a foreign person, either inside or outside the United States, without first obtaining proper export authority. Violators of ITAR and/or EAR are subject to civil and/or criminal fines and penalties under 22 U.S.C. 2778 and 50 U.S.C. 2410. Recipient shall include this notice on any reproduced page or portion of a page of this document.

L3 communications
Communication Systems-East

Communication Systems – East
1 Federal Street
Camden, NJ 08103-1013

K00017992, Rev A.

Before You Start

This document describes the electronic rekey process for keys on a Talon (KOV-26) network encryptor. This process presumes that you have had an initial load of either operational or seed key material and want to update or activate those keys. Initial keys can be acquired from the EKMS Central Facility (CF) using Talon Key Order Request Form 1090. Before completing the key order form, please contact the EKMS CF's help desk (1-800-635-5689) so that they can ensure you are authorized to order key (i.e. You have a User Representative account and have been authorized the required key ordering privileges).

An electronic rekey is used for two purposes – to update operational keys and to activate seed keys. Users with operational key should perform the electronic rekey at least once a year to ensure your keying material does not expire, however quarterly electronic rekeys are recommended for the purpose of obtaining the latest Compromised Key List -CKL. Users with Seed Key must perform an electronic rekey to convert a seed key to an operational key before they can use the device for communications.

A rekey is accomplished by making a secure data call to the EKMS Central Facility electronic rekey system. To do this, you MUST have either a Seed Key or Operational Key that has been assigned to the SCIP protocol (see Figure 1 below).. When the call is placed, a secure data session (using the SCIP key) will automatically be established. During this rekey session, all SCIP and HAIPE keys will be rekeyed.

In addition to having the necessary keys, the user performing the key update must be privileged to do so by the Site Security Officer. Both Load Key and Modem privileges must be assigned. See Figure 2.

Figure 1 Talon Manage SDNS Key window

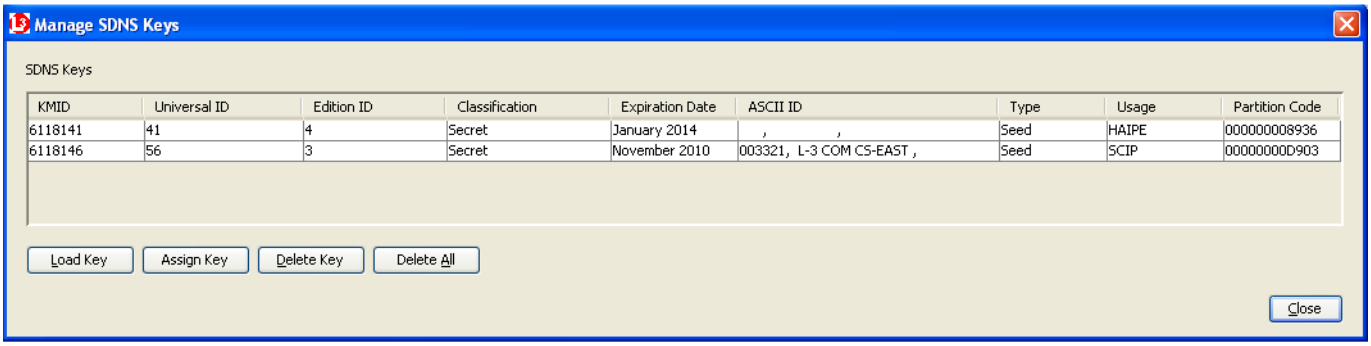
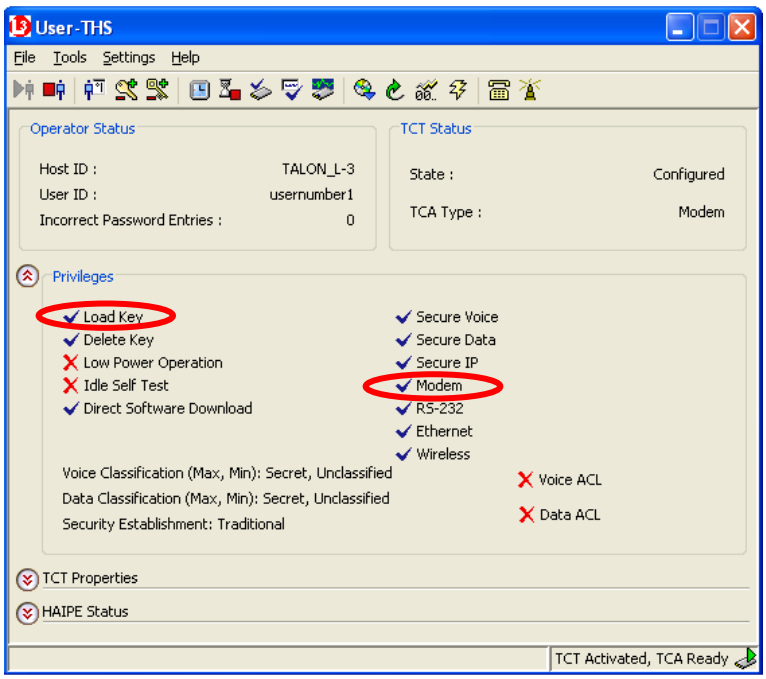


Figure 2 – Talon User Permissions Screen



Electronic Rekey Process

1. Insert the Talon card into the host computer, and connect the Modem Adapter (Figure 3).

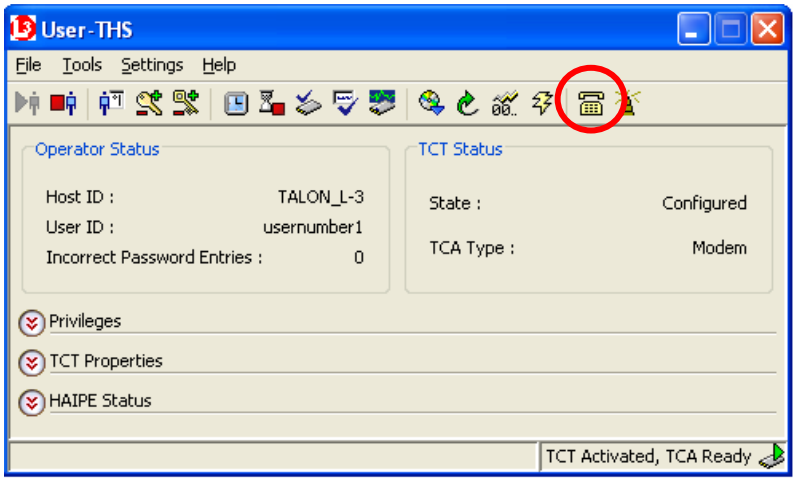
Figure 3 – Talon Card and Modem Adapter

2. Log on to the Talon with the User THS and the Modem adaptor connected (Figure 4).

Figure 4 – Talon Login Screen

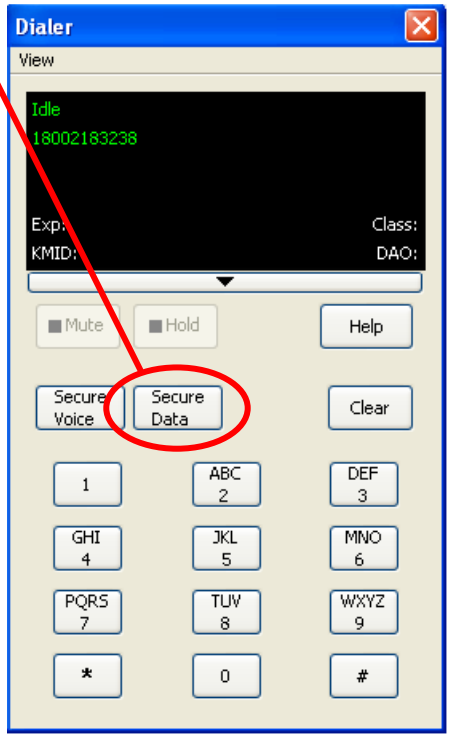
3. Connect the Modem to an analog phone line and bring up the Dialer window by clicking on telephone symbol (Figure 5).

Figure 5 – Talon Status Screen – Dialer access



4. Dial the Central Facility (KMC) rekey number (**800-218-3238 or 410-526-3444**). There will be no voice prompt. Select Secure Data (Figure 6).

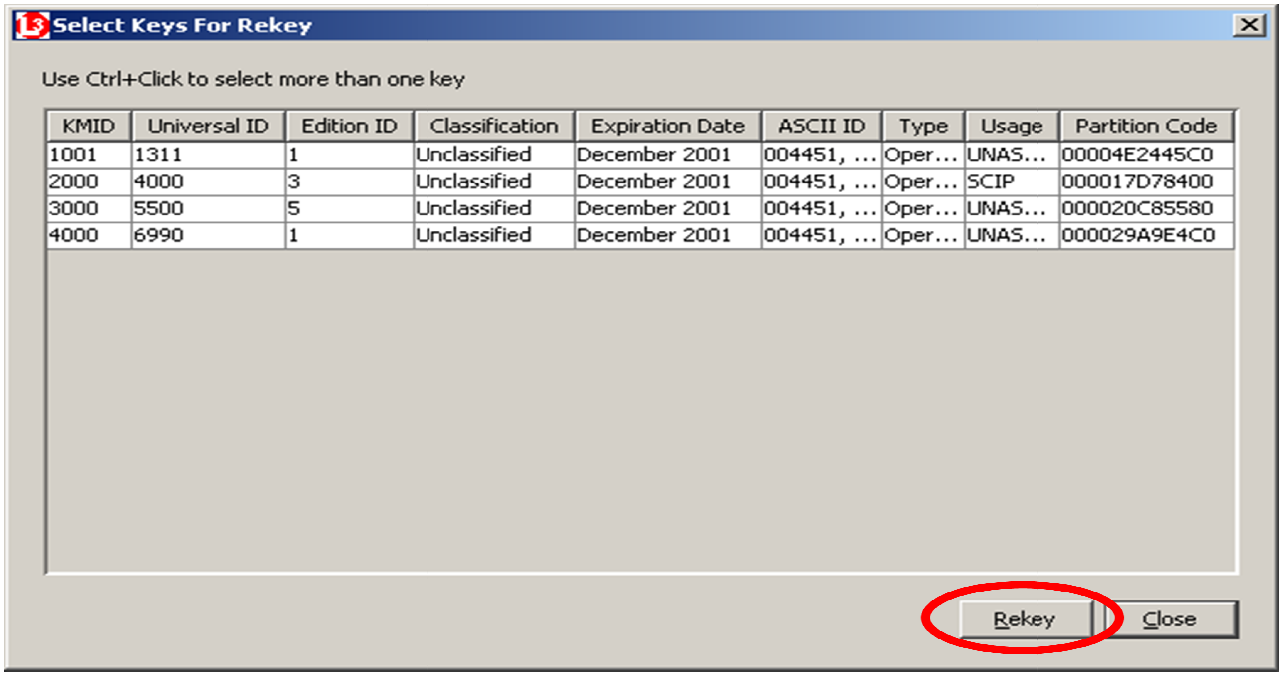
Figure 6 – Talon Dialer Screen



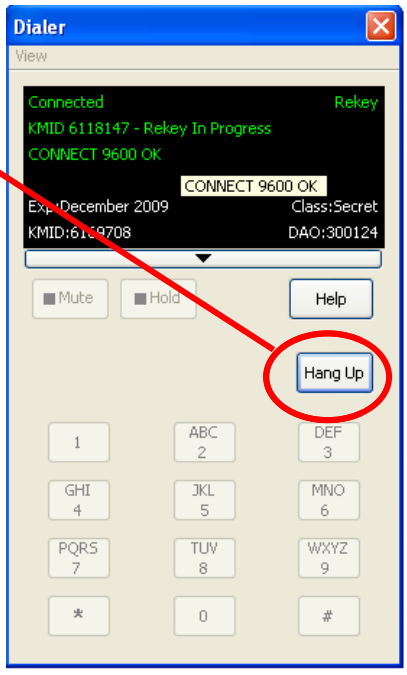
5. KMC will initiate "go secure" and start the rekey.

Figure 7 – Rekey in Process

6. Select SDNS Key(s) for Rekey
    - Left mouse click on a row
    - Hold Ctrl key to select multiple rows



7. When Rekey Complete, disconnect the call.



8. Check the status of the keys by selecting Manage SDNS Keys (Figure 8 &Figure 9).

Figure 8

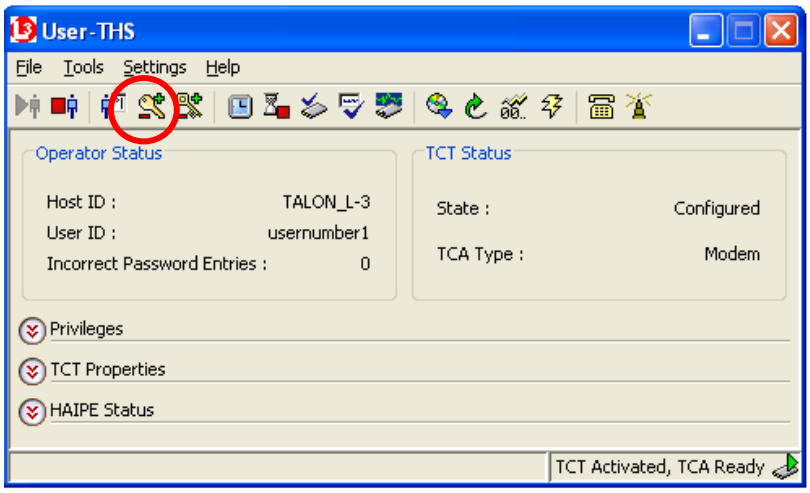


Figure 9